COMPUTER SYSTEM SECURITY AND
PRIVACY ADVISORY BOARD
SUMMARY OF MEETING

National Institute of Standards and Technology
Gaithersburg, MD
September 12-14, 2000

Action items are highlighted in BOLD/ITALIC text.

Tuesday, September 12, 2000

Board Chairman, Franklin S. Reeder, convened the Computer System Security and Privacy Advisory Board for its third meeting of the year at 9:10 A.M.

Board members present in addition to the Chairman were:

Mr. Peter Brown
Mr. Richard Guida [9/13&14]
Mr. Daniel Knauf
Mr. Stephen Lipner
Mr. John Sabo
Prof. George Trubow
Mr. James Wade
Mr. Rick Weingarten [9/13&14]
Ms. Karen Worstell

The entire meeting was open to the public. There were seven people from the public in attendance when the meeting was called to order.

Mr. Ed Roback, Board Secretary reviewed the agenda and the handout materials for the meeting. He also reported that there was no activity on the FY01 budget as it was still awaiting Congressional action.

Opening Remarks by Chairman
Franklin S. Reeder

Chairman Reeder addressed the recent report issued by Representative Steven Horn giving grades to federal agencies computer security programs. The Board may wish to issue a statement expressing their point of view on this issue. Also, as a result of the upcoming Administration changes, the Board should consider development of its own platform on computer security and privacy issues to make available to the transition team.

Other members input at this time included discussion by John Sabo on the efforts of the International Security and Trust Privacy Alliance in developing a privacy framework of services. He asked if the Board would be interested in sponsoring a springtime conference built around solutions to privacy. ***Chairman Reeder will contact GSA to see if the Board can, as a Federal Advisory Committee, sponsor conferences/workshops, etc*.** Other members of the Board agreed that this type of activity would be worthwhile and a valuable asset to the Board in accomplishing its mandate.

Board Member Dan Knauf mentioned that the April 2001 conference of the NSTISSC would focus on addressing the major issues for the transition team. ***He said that he would check with the planning coordinator, Art Money, about the possibility of the Board participating with NSTISSC.***

Security Metrics Workshop – Next Steps

Fran Nielsen, NIST

Dr. Nielsen presented an overview of the draft report "Approaches to Security Metrics" which was the report of the workshop held on June 13-14, 2000, at NIST in conjunction with the CSSPAB meeting. Board members expressed their thoughts on the next phase that this report could take. A possible addendum could be attached to the current report to reflect changes in certain issues since the workshop occurred. It would also be useful to obtain the input of those who were unable to attend the original workshop. Creation of a web page on security metrics issues on the CSSPAB website was suggested. It could become a repository for identified areas of metrics and could perhaps lead to the development of a set of metrics that agencies and organizations could use to gauge how they stand. A website-based exchange forum could be established to include discussion of what people see as the pros, cons, benefits, etc. of using a security framework. ***Dr. Nielsen will work with the Division staff on the creation of such a website activity***. ***Board members were asked to provide any comments to Dr. Nielsen on the current draft***.

Project Matrix

Glenn Price, Critical Infrastructure Protection Office (CIAO)
Michael Lombard, Department of Commerce (DOC)

Glenn Price of the CIAO began his briefing with background information on the formation of Project Matrix. The activity was developed as a result of the PDD63 directive. In February 200, the General Services Administration, Office of Management and Budget and the National Security Council gave their support to the Project Matrix effort to work with agencies to identify their critical infrastructures. Additionally, the Departments of Commerce, Treasury, Energy, Health and Human Services and the Social Security Administration are participating in the effort. Nine other agencies are also expected to join in soon. The project is housed at the Department of Commerce and operates under the CIAO. The Secretary of Commerce, Norman Mineta is very supportive of this activity.

Project Matrix is designed to identify and accurately characterize all the assets, nodes, networks, associated infrastructure dependencies required for the government to fulfill its national security, national economic security, and critical public health and safety responsibilities. Mr. Price identified three steps for matrix building: (1) determine which assets are relevant; (2) capture the major nodes and networks upon which the US government is most dependent; and (3) tie the most critical assets and their supporting nodes and networks to underlying infrastructures.

The Department of Commerce served as the prototype for this effort and provided the proof of concept testbed for Project Matrix. Mr. Mike Lombard, DOC, briefed the Board on the DOC participation results. He said that they had identified three DOC programs as critical assets dependent infrastructures. They included NIST's time, scale and frequency standard and dissemination system and the Tropical Storm Prediction Center/National Hurricane Center of NOAA.

The benefits of this matrix approach, said Price, is that it supports the U.S. government's general information technology security, counter intelligence and counter terrorism programs. Project

Matrix will facilitate better public sector compliance and private sector cooperation in the implementation of PDD63. The project has been well received by Congressional representatives.

Chairman Reeder asked Mr. Price how the Board could help the efforts of Project Matrix. Mr. Price replied that there is a need to convince people to look at things in the aggregate rather than on an agency-by-agency basis. He said that the Board could be supportive by becoming an advocate and publicly support this effort.

Board Discussion on Focus Paper on Security Metrics

Karen Worstell, Discussion Leader

Karen Worstell's discussion focused on security metrics issued that she had raised at the June workshop. The points were the establishment of cross agency governance, establishment of an approach of baseline controls, adoption of a national standard for information security management, use of hybrid production/maturity models, establishment of a federal/private sector best practice sharing, focusing on security as the value added capability to moving to the web, expansion of the scope of GAO audits, establishment of the operational context of information security in respective agencies according to their business mission, and the use of metrics to measure trends.

She sees activity in some of these areas such as the action being taken to create a federal government CIO. She suggested that a baseline control effort be enhanced by following the example of those used by the insurance industry and their need to rate risk. Criteria are needed to insure security as a value. Brand valuable and consumer confidence are two essential measures to protect and create value. There is the need to convince others that funding is needed for security because of the value it can create. Cases can be made that security pays for itself. Karen offered several examples where this type of investment had been of benefit. She also said that a recent Forrester Report stated that there was a lost of $2.8B last year because of consumers concerns of how companies handled data provided online.

Board Discussion on Maturity Framework Document of the CIO Security, Privacy and Critical Infrastructure Committee

John Sabo, Discussion Leader
Steve Lipner, Discussion Leader
Marianne Swanson, Discussion Leader

John Sabo began the briefing with an overview of the draft document. The general observation by John and Steve Lipner was that the document was very high level with little tie to the objective of system security. They identified levels 4 and level 5 has only mentioning vulnerabilities and threat and that it was not apparent from the framework that a level 4 or level 5 agency would meet intuitive definitions of security. They concluded that the government agencies need security now, metrics must be security and not weight of plans, and the focus must be on effective, scalable security measures and management metrics. They recommended that there be defined security basics or baseline controls and that agencies focus their attention on implementation and tactical plans. [ref.1] Marianne Swanson of NIST said that it was possible that another version of this document would be issued that offered different approaches to this type of concern. It was also mentioned that NIST may put together a companion document to cover areas such as how to do all of the assessments, develop baselines, and answer the question of what happens to the self-assessment data and how all of this information is useful.

Chairman Reeder suggested that the Board draft a letter to be sent to Mr. Gilligan, Chair of the CIO Committee, stating the Board's observations and recommendations.

Issues and Future Direction of CSSPAB

Dan Knauf, Discussion Leader

Mr. Knauf presented an overview of issues and future directions for the Board to consider. [ref. 2] The overall consensus of the Board was that they should be more proactive. Mr. Knauf's briefing offered tactics and approaches to accomplishing these goals.

One of the issues that the Board could focus on is the knowledge that there is not a civilian sector effort on information assurance issuances such as there is on the classified side. This could be brought to the attention of the Congress. Other areas of opportunity suggested were the pending changes in Congress and transition of the new Administration. The Board could choose to act on several major issues such as cross-agency governance, baseline security and accountability issues. Another issue that the Board could weigh in on is whether Congress is organized, structured, and run in an effective way to deal with digital revolution issues and security and privacy. The recent Horn report card on computer security of federal departments and agencies is also an opportunity for the Board to offer opinions and recommendations. ***Peter Browne offered to draft a response to Congressman Horn's Report Card issuance.***

There will be continued discussion of these issues at future meetings.

The meeting was recessed at 4:40 p.m.

Wednesday, September 13, 2000

Chairman Reeder reconvened the meeting at 9:10 a.m. Board member, Steve Lipner invited the Board to hold their December meeting at the Microsoft headquarters in Redmond, WA in conjunction with a Security Summit held at Microsoft that same week. The Board accepted his invitation. The Board meeting will be held on December 4, 5 and until noon on December 6. The Microsoft Security Summit will begin on the afternoon of December 6 and December 7 and 8.

Discussion of Board Agenda/Work Plan

Franklin Reeder, Discussion Leader

Chairman Reeder led a discussion on how the Board can make a difference and the areas that the Board believes to be important. He summarized the actions from the first day of the meeting. They included: the need for building on the metrics workshop and its output; the need for business case metrics and the consequences of not having them form the business case; the structure of the civilian side of the Executive branch; interaction with the CIO council; response to the Horn Report Card; and the Board's collateral responsibility to be involved in the NIST's computer security program and weigh in with advice on what the Board believes the priorities of the program should be.

Immediate deliverables of the Board should be a response to Gilligan/CIO Council on the framework document and the cross governance issues. Steve Lipner stated that privacy issues are a growing critical factor. How is the Government Paperwork Elimination Act affecting the federal government and how have agencies responded to it thus far. ***Rich Guida volunteered to develop a discussion paper on this issue. George Trubow also offered assistance if there was any survey research that needed to be done.***

Chairman Reeder asked if there is any way that the Board could get some data on federal spending for computer security and benchmark that data back to what is actually being spent. It would be useful to be able to have one or two areas that could be compared to the private sector such as comparing what is spent by the Social Security Administration and Aetna. Mr. Reeder also suggested that the Board members broaden their outreach to see what others see are the real problems. Do others believe that the Executive branch is asking for enough information about computer security programs of the agencies?

Rick Weingarten would like to see the Board invite more Congressional members/staffers to meetings and ask them what the Board could do for them. Rich Guida agreed with this especially as new computer security and privacy legislation is being issued.

OMB Update

Glenn Schlarman
Office of Information and Regulatory Affairs (OIRA), OMB

Mr. Schlarman began his briefing by recognizing the excellent work efforts of Fran Nielsen and Marianne Swanson of NIST while they were serving on details to the OIRA.

Since the June Board meeting, OIRA has been focusing on the survey of the 43 high impact programs identified as a result of the Y2K effort. The OMB point of contact for this effort is Kamela White. John Spottila' testimony at the September 11th hearing on Report Card on Computer Security in the Federal Government before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform outlined the findings in a very general way.

Next, Glenn briefed the Board on the status of some pending security related legislation. He said that S. 1993, the Government Information Security Act of 1999, appears to be having some difficulty in conference. H.R. 2413, the Computer Security Enhancement Act, doesn't appear to have a strong enough foundation at this juncture. There are also several pieces of legislation on the subject of a Federal CIO being circulated on the Hill. Glenn pointed out that the Deputy Director for Management within the Office of Management and Budget is the current Federal CIO, and he believes that carving out information technology from this office would weaken the effort.

In the information technology effort, OMB measures at the executive level and at the broader programmatic level. There are 26,000+ mission critical systems within the federal government. OMB needs to ensure that agencies are continuing to assess their systems, and agencies need to know that OMB's expectation is that these assessments will be ongoing.

On the topic of Congressman Horn's Report Card, OMB liked the attention the grading brought to the computer security issue. He encouraged the Board to raise their concerns to the attention of senior management.

Next, Mr. Schlarman reported on the status of budgetary proposals for FY2001. He said that there was a 15% increase for security and CIP budget over last year. The National Plan budget chart showed 90% of these dollars been directed to the Department of Defense. The FY2002 budget outlook is unclear. Cross cutting initiatives are having a very difficult time obtaining funding and there are some turf struggles happening.

The Board was encouraged to develop a relationship with influential staffers and Congressional representatives as a way to strengthen the Board's mandate.

Overview of Activities of BITS Technology Group for the Financial Services Roundtable

Catherine Allen, Chief Executive Officer, BITS
Faith Boettger, Senior Director, BITS

Ms. Allen presented an overview of the BITS mission and initiatives. [ref. 3] BITS mandate is to facilitate the growth of electronic commerce, sustain consumer confidence and trust by ensuring the safety, soundness, privacy and security of financial transactions. The focus is 80% on electronic commerce issues and 20% on payment related issues. The BITS Board of Directors consists of 20 heads of the largest institutions and banking industry. Founding Board of Directors Members Emeritus include Edward Crutchfield, Chairman of First Union Corporation, Spencer Eccles, Chairman and CEO of First Security Corporation, Paul Hazen, Chairman of Wells Fargo and Company and Terrence Murray, Chairman and CEO of Fleet Boston Financial Corporation. There is a 'kitchen cabinet' group of 33 of the most senior people in technology in the United States. They meet monthly via teleconferences. The Board of Directors meets twice a year and conducts numerous conference calls throughout the year. BITS is a sister organization of the financial services roundtable which is a lobbying organization. They manage over 35 committee efforts each year that included over 800 meetings/conference calls annually.
There are eleven active initiatives being handled by a staff of 14 members. They cover aggregation services, business-to-business e-commerce framework, wireless technologies, service providers/outsourcers business practices, electronic (digital) signature and records legislation, and security and risk assessments.

Faith Boettger spoke to the Board on the BITS Financial Services Security Lab. It is a testing facility that tests products and services that strengthen the security of electronic payment systems and related e-commerce technologies.

The Board thanked them both for their briefings and identified a need to follow-up on their metrics activities, especially in the wireless area.

Emerging Trends in International Privacy Law

Jeffery Ritter, Esq.
Kirkpatrick and Lockhart LLP

Mr. Ritter works in the Washington, DC offices of Kirkpatrick and Lockhart, LLP. He has over two decades of experience as a commercial lawyer and has been a pioneer in defining the emerging law of electronic commerce. Based on his knowledge of emerging trends in international privacy laws, the emphasis of his presentation to the Board was to offer assistance to them on how best to recommend/design a national privacy policy. [ref. 4] He shared a recent paper he co-authored on the subject of emerging trends in international privacy law. He points to the two legal models for privacy rules: generic architecture and sectoral model. He also reviewed the core principles of privacy law. Mr. Ritter stated that Safe Harbor was declared ineffective by 30 of the top 50 Fortune 500 companies. In round 2 of the Safe Harbor effort, Treasury is working with the European Community to develop the plans to address and protect the financial communities concerns. He recommended that this Board encourage a continued dialogue with the legal community so that those who are making the rules are sensitized to the technology so that good public policy happens.

INFOSEC Research Council R&D Agenda – An Update

Carl Piechowski, Chairman, Infosec Research Council
Carl Landwehr, Executive Agent, Infosec Research Council

The INFOSEC Research Council (IRC) is an informal group consisting of government sponsors of information security research from the Department of Defense, the Intelligence Community and federal civilian agencies. [ref.#5] It is not formally chartered under any specific organization. It is a vehicle for sharing information between different people in different organizations. The IRC targets the federal R&D managers and offers a 'bigger picture perspective.' They hold bimonthly meetings that include program discussions, relevant technical presentations, and review of new developments and announcements of current/upcoming events. They also have a INFOSEC Science and Technology Study Group (ISTSG). Recent meeting topics have included program briefs on DARPA Information Assurance Science and Engineering Technology program, IC Computer Network Threat Panel, Sandia INFOSEC R&D, etc.

Carl Landwehr spoke to the Board on the INFOSEC Research Hard Problem list. The purpose of this activity is to identify important roadblocks to effective information security, guide research program planning and achieve consensus on priorities. This is achieved by discussion and email exchanges among members and contributions from national experts.

Public Participation

Mr. Gideon Samid of D&G Sciences, McLean, VA spoke to the Board during the public participation segment. He raised the issue of the vulnerability to encryption breakdown and penetration of our encryption systems. It is his opinion that inherent weaknesses are not being addressed and that the United States is most vulnerable to a cyber attack. He asked that the Board consider his concern and make it one of their priorities.

The Chairman recessed the meeting at 4:50 p.m.

Thursday, September 14, 2000

Chairman Reeder reconvened the meeting at 9:10 a.m.

Board Discussion on Privacy Awareness Issues

Rick Weingarten, Discussion Leader

Mr. Weingarten opened his discussion with the proposal that the Board conduct a privacy workshop, such as they did on security metrics. June 2001 was the suggested timeframe for conducting the workshop. It should be held in the Washington, DC area and a request for invited papers would be issued. ***The Board Secretariat staff will look at the availability of meeting locations for that time period.***

It was suggested that the workshop be more focused on specific privacy issues. The scope of the workshop could cover federal privacy policy. This includes primary policy for the federal collection, holding and use of personal information, federal negotiation with the international community and privacy conflict with other federal concerns about cybercrime. There is also the issue of re-examining the Privacy Act itself that could be addressed. It is 25 years old. Is it currently adequate given the new wave that we are experiencing in the privacy area? Perhaps it could be examined in three phases. First, within the frame of existing statutes that deal with the issues GPEA raises, second, what is it that cannot be dealt with within the existing policy and the third phase is the possible re-write of the Privacy Act itself. It was also suggested that the Board share these findings/concerns with Congressional committees identifying that we believe this is a matter that should be addressed on the Congressional agenda. Another question raised was do we need an electronic privacy act.

George Trubow and Rick Weingarten volunteered to draft a discussion paper on these issues for action at the December Board meeting. This draft would include advice and input for a transition team transmittal from the Board.

Rick Weingarten is to develop a work plan for the proposed June privacy workshop.

Summary of Board Discussions and Follow-on Actions

1. ***Review the NIST Computer Security Division program in two phases;*** one-hour overview of the FY2001 program at the December meeting; FY2002-FY2003 projected budgets discussion at the March 2001 meeting. Include an overview of the NIAP effort, bringing in user constituents and vendors to brief.

2. Establish a list of principles and values of the Board. ***Dan Knauf and Peter Browne will work on a first draft of this list of principles and values/tenets for review by the Board at the December meeting.***

3. NIST to develop an information forum/website on the subject of security metrics***. Fran Nielsen will work with the Computer Security Division webmaster on this effort.***

4. The Board identified the need to have someone gather data about what happens when you don't have a trusted system. Invite the National Science Foundation to brief the Board on what their electronic research agenda is. Also, invite the National Research Council to brief on what they are currently doing in this area. ***Rich Guida will draft a set of questions to ask each of these agencies to cover in their briefings to the Board.***

5. Questions were raised regarding website vulnerabilities. How do you know who you can trust once you have found what you are looking for? How do agencies insure that they are delivering to the people? How do they know that messages are not being altered in transition or when they are downloaded? It was suggested that the Board could commend NIST to develop guidance on website vulnerability that addresses these issues***. Rich Guida volunteered to produce a draft on the specific interest areas and from comments received from the members, develop a proposal to NIST.***

6. Metrics workshop follow-on included comments on the draft report produced by Fran Nielsen. ***Board members were asked to provide any feedback to her by September 30. It was suggested that a taxonomy of the different approaches be included in the report. Dr. Nielsen will provide the members with a revised draft to include the taxonomy.***

7. ***It was recommended that the Board develop portions of the security metrics comments produced by Karen Worstell into Board recommendations.***

8. Additional follow-up metrics activities included getting input from those who were unable to attend the metrics workshop. It was also suggested that for the December meeting, the Board invite those persons who have knowledge of best practices, baseline controls and security metrics. A half-day session could be devoted to these discussions. Steve Lipner mentioned that many of the invitees to the Microsoft Summit would have this experience and could possibly be contacted to address the Board. ***Fran Nielsen and Steve will work together to develop an appropriate agenda.***

9. *The draft letter to John Gilligan was reviewed and will be sent to Mr Gilligan in advance of going final.*

10. The Board agreed on essential points of the proposed draft letters to be sent to Congressman Horn. ***The Chairman will produce a final document for the Board's consideration***.

There being no further business, the meeting was adjourned at 12:30 p.m.

Ref. 1. Sabo and Lipner presentation
Ref. 2. Knauf outline
Ref. 3 Allen presentation on BITS
Ref. 4. Ritter presentation
Ref. 5. Piechowski/Landwehr presentation

Edward Roback
Board Secretary

CERTIFIED as a true and accurate summary of the meeting.

Franklin S. Reeder
Chairman

.